IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Adrian Alvarez Diez

Serial No.:   10/562,488

Filed: December 22, 2005

Group Art Unit: 2458

Confirmation No.:   6307

For: METHOD AND SYSTEM FOR AUTHENTICATING SERVERS IN A DISTRIBUTED APPLICATION ENVIRONMENT

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

APPEAL BRIEF IN SUPPORT OF APPEAL
FROM THE PRIMARY EXAMINER TO THE BOARD OF APPEALS

In response to the Notification of Non-Compliant Appeal Brief that was mailed May 19, 2010, Applicants submit a replacement portion for the Summary of Claimed Subject Matter portion of the Appeal Brief, in compliance with 37 CFR 41.37.

5. Summary of Claimed Subject Matter

Appellant is appealing from the Examiner's rejection of claims 1-19. Claim 1 is an independent claim. Claims 2-6 and 17 depend directly or indirectly from claim 1. Claim 7 is an independent claim. Claims 8-11 depend directly or indirectly from claim 7. Claim 12 is an independent claim. Claims 13-15 and 18 depend directly or indirectly from claim 12. Claim 16 is an independent claim. Claim 19 depends directly from claim 16.

Claim 1 is directed at a method for authenticating a third tier server system in a distributed application environment (e.g., *abstract; pg. 6, lines 12-28)*. The distributed application environment comprises a client system having parts of the distributed application, server systems having the remaining parts of the distributed application, and third tier server system which exchanges data between said client system and said server systems *(e.g., pg. 6, lines 12-28; Figs. 2A, 4-5)*. The client system acts as single point of recognizing and managing third tier server certificates and provides access to a common data base of the distributed application environment which contains third tier server certificates received from said third tier server which have been accepted as trustworthy for the distributed application environment *(e.g., pg 10, line 26 - pg 12, line 6; pg. 16, lines 10-12)*. Claim 1 further requires that, at said server systems side, the method comprise: receiving from said common database of said client system at least all necessary information of a third tier server certificate being accepted as trustworthy for determining to accept or to decline a connection to said third tier server *(e.g., pg. 6, lines 12-28; pg. 10, line 26 - pg 11, line 19; pg. 12, lines 7-20; pg. 14, line 13 - pg. 15, line 15)*, comparing said received at least all necessary information with a server-copy of the third tier certificate received from said third tier server system *(Id.)*, accepting said third tier server system as to be authenticated if said at least all necessary information matches said server-copy of the third tier certificate *(Id.)*

Claim 7 is directed at a method for authenticating a third tier server system in a distributed application environment (e.g., *abstract; pg. 6, lines 12-28)*. The distributed

application environment comprises a client system having parts of the distributed application, server systems having the remaining parts of the distributed application, and a third tier server system which exchanges data between said client system and said server systems *(e.g., pg. 6, lines 12-28; Figs. 2A, 4-5)*. The client system provides access to a common data base of the distributed application environment which contains third tier server certificates received from said third tier server which have been accepted as trustworthy for the distributed application environment *(e.g., pg 10, line 26 - pg 12, line 6; pg. 16, lines 10-12)*. Claim 7 further requires that, at said client system, the method comprise: receiving a client-copy of a third tier server certificate from a third tier server system *(e.g., pg. 6, lines 12-28; pg. 10, line 26 - pg 11, line 19; pg. 12, lines 7-20; pg. 14, line 13 - pg. 15, line 15)*, determining whether said received client-copy of said third tier server certificate can be accepted as trustworthy *(Id.)*, storing said client-copy of said third tier server certificate in said common data base of the distributed application environment if said client-copy of said third tier server certificate has been accepted as trustworthy *(Id.)*, and transferring to each server of said server systems at least all necessary information of said client-copy of said third tier server certificates being accepted as trustworthy for determining to accept or to decline a third tier server system *(Id)*.

Claim 12 is directed at a system for authenticating a third tier server system in a distributed application environment (e.g., *abstract; pg. 6, lines 12-28)*. The distributed application environment comprises a client system having parts of the distributed application,-and application server systems having the remaining parts of the distributed application *(e.g., pg. 6, lines 12 - 28; Figs. 2A, 4-5)*. Claim 12 further requires the application server systems-comprise a transfer server component which, in a first computer process, supports non-continuous and secure client-server connection for receiving certificate information from a client of a third tier server certificates being accepted as trustworthy for determining to accept or to decline a connection to said third tier server system (e.g., *pg. 10, lines 19-22; Fig. 2C, element 120)*, a connection negotiator component which, in a second computer process receives incoming third tier

server certificates via a secure connection between said application server systems and said third tier server (*e.g., pg. 10, lines 3-5; Fig. 2C, element 140*), and a certificate verifier component which, in a third computer process, compares said third tier server certificate received from said third tier server with said certificate information received from said client (*e.g., pg. 10, lines 6-10; Fig. 2C, element 130*).

Claim 16 is directed at a client system for authenticating third tier server in a distributed application environment (e.g., *abstract, pg. 6, lines 12-28*). The distributed application environment comprises a client system having parts of the distributed application, application server systems having the remaining parts of the distributed application (*e.g., pg. 6, lines 12-28; Figs. 2A, 4-5*). Claim 16 further requires that the client system comprise a connection negotiator component which, in a first computer process, receives incoming third tier server certificate via a secure connection from said third tier server (*e.g., pg. 8, lines 18-20; Fig. 2B, element 60*), a common data base of the distributed application environment which, in a second computer process, stores said third tier server certificates received from said third tier server system which have been accepted as trustworthy for the distributed application environment (*e.g., pg. 9, lines 5-8; Fig. 2b, element 4*), a certificate verifier component which, in a third computer process, compares said received third tier server certificate with information stored in said common database and stores them into said common database if it matches (*e.g., pg. 8, lines 21-24, Fig. 2B, element 50*), a user interface component which, in a fourth computer process, allows for accepting or rejecting an unknown third tier server certificate not contained in said common data base (*e.g., pg. 8, lines 25-27; Fig. 2B, element 40*), and a certificate transmitter component which, in a fifth computer process, generates certificate information of said third tier server certificates being accepted as trustworthy for determining to accept or to decline a third tier server from said common database and transmits them to said application server systems via a secure connection (*e.g., pg. 9, lines 1-4; Fig. 2B, element 30*).

For each of the foregoing reasons, Appellant submits that the Examiner's final rejections of claims 1-19 were erroneous, and respectfully requests reversal of these decisions.

Respectfully submitted,

By: _____
Grant A. Johnson
Registration No.: 42,696
IBM Corporation - Department 917
3605 Highway 52 North
Rochester, Minnesota 55901-7829

Date:

Telephone: (507) 253-4600
Fax No.:   (507) 253-2382